Best Practices in Enterprise IAM

Liza Lowery Massey

Montana Government IT Conference

December 6, 2007

The Issue

- More sensitive & confidential data is being stored on-line
- We are under attack
- Securing the enterprise is expensive
- Security procedures can be counter-productive
- Management understanding & support is lacking

The Solution

- Assess and manage your risks
- Know your data
- Implement an IAM Program
  - Processes, technologies & policies
  - Managing digital identities
  - Controlling how identities grant access

Assess & Manage Risk

- What is likely to occur?
- What is the impact if it occurs?
- What mandates exist?
- How secure do we need to be?
- What should we do first?
- What resources do we have/need?

Know Your Data (classification)

- Understand applicable state & federal laws
- Follow best practices
- Form a cross-organizational team
- Draft your policy
- Run it by legal
- Gain approval
- Educate the organization

IAM Programs

- Drivers
  - Fear
  - Compliance
  - Improvement
- Challenges
  - Fragmentation
  - Funding
  - Balance

IAM Programs

- Success Factors
  - Return on Investment
  - Governance
- Technical
  - Areas to Address
  - Standards
  - Best Practices

Areas to Address

- ID administration & provisioning
- Host based access control
- Extranet access control
- Single sign on
- Biometric/strong authentication
- Web services access management
- Mainframe access control
- Monitoring and auditing

Standards

- LDAP
  - Lightweight Directory Access Protocol
  - Networking protocol for querying and modifying directory services
  - Running over TCP/IP
- SAML
  - Security assurance markup language
  - XML for IAM over the Web
  - Critical middleware solution for state and local governments

Best Practices

- Availability
- Authentication
- Integrity
- Confidentiality
- Non-repudiation
- Compliance

Getting Started

- Establish governance
- Allocate resources
- Designate a responsible party
- Prioritize needs
- Draft & distribute policies
- Review & modify business processes
- Plan a phased implementation
- Identify & deploy technology

The Next Step

- Merging physical and logical security
  - Consolidate responsibility
  - Example – smart card
    - Electronically identifies a person
    - Serves as a visual badge
    - Grants access to facilities
    - Part of 2 or 3 tier access to IT applications & data

Related Reading

- *I Am Who I Say I AM*
  - http://www.centerdigitalgov.com/publications.php

Liza Lowery Massey
The CIO Collaborative

liza@ciocollaborative.com
www.ciocollaborative.com
702-743-4634